AMENDMENTS TO CLAIMS

Claims 1 - 43 (cancelled)

Claim 44 (original): A method for black box analysis of a device capable of accessing protected content, the method comprising:

providing a device to be analyzed;

inputting to the device a data item comprising encrypted protected content and a plurality of encrypted versions of a content key for accessing the protected content, each of the plurality of encrypted versions being encrypted in accordance with a different one of a plurality of group keys;

receiving, from the device, decrypted content representing a decryption of the protected content;

determining whether the received content is one of the following: erroneous; and null, and producing a result;

identifying a set of group keys comprising at least one group key which is known to the device based, at least in part, on the result,

wherein the data item also comprises at least one invalid content key encrypted in accordance with one of the plurality of group keys.

Claim 45 (cancelled)

Claim 46 (original): A method according to claim 44 and also comprising performing the following steps at least once before performing the identifying step:

choosing a new plurality of encrypted versions of the content key; and

performing the inputting, receiving and determining steps.

Claim 47 (original): A method according to claim 46 and wherein the choosing a new plurality step comprises choosing based, at least in part, on at least one of the following:

at least one result of the determining step performed before the choosing step; and

the plurality of encrypted versions of the content key used in the inputting step performed before the choosing step.

Claim 48 (original): A method according to claim 44 and wherein the identifying step comprises identifying the one of the plurality of group keys with which the invalid content key is encrypted.

Claim 49 (original): A method according to claim 44 and wherein the identifying step comprises identifying a group key which is not one of the plurality of group keys with which the invalid content key is encrypted.

Claim 50 (original): A method according to claim 44 and wherein the identifying step comprises identifying a group key which is one of the plurality of group keys with which the invalid content key is encrypted.

Claim 51 (new): A method for black box analysis of a device capable of accessing protected content, the method comprising:

providing a device to be analyzed;

inputting to the device a data item comprising encrypted protected content and a plurality of encrypted versions of a content key for accessing the protected content, each of the plurality of encrypted versions being encrypted in accordance with a different one of a plurality of group keys;

receiving, from the device, decrypted content representing a decryption of the protected content;

determining whether the received content is one of the following: erroneous; and null and producing a result;

identifying a set of group keys comprising at least one group key which is known to the device based, at least in part, on the result,

wherein the data item also comprises at least one invalid content key encrypted in accordance with one of the plurality of group keys, and

the protected content is protected in accordance with the following method:

providing a plurality of authorized devices;

dividing the plurality of authorized devices into a plurality of groups, each of the plurality of authorized devices being comprised in at least one of the plurality of groups, no two devices of the plurality of authorized devices being comprised in exactly the same groups;

determining whether at least one device of the plurality of authorized devices is to be prevented from having access to the protected content and, if at least one device is to be prevented, removing all groups comprising the at least one device from the plurality of groups, thus producing a set of remaining groups; and

a4

determining an authorized set comprising groups from the set of remaining groups, such that each device of the plurality of authorized devices which was not determined, in the determining whether, to be prevented from having access is comprised in at least one group of the authorized set.

Claim 52 (new): The method according to claim 51 and also comprising:

assigning, to each one of the plurality of authorized devices, a set of keys comprising one group key for each group of which the one device is a member; and

utilizing at least some of the group keys for communication of a content decryption key to at least one of the plurality of authorized devices.

Claim 53 (new): The method according to claim 52 and wherein the utilizing comprises, for each of the plurality of authorized devices:

obtaining the content decryption key, wherein the obtaining comprises performing no more than a predetermined number of decryptions.

Claim 54 (new): The method according to claim 52 and wherein the utilizing comprises, for each of the plurality of authorized devices:

obtaining the content decryption key, wherein the obtaining comprises performing exactly one decryption.

Claim 55 (new): The method according to claim 52 and also comprising:

at each authorized device having access to the protected content, performing no more than a predetermined number of decryption operations, said predetermined number being the same for all authorized devices, to obtain the content decryption key from an encrypted form thereof, said encrypted form being encrypted with a group key corresponding to a group of which said authorized device is a member.

Claim 56 (new): The method according to claim 55 and wherein said predetermined number does not depend on the number of authorized devices.

Claim 57 (new): The method according to claim 55 and wherein said predetermined number is equal to 1.

Claim 58 (new): The method according to claim 52 and also comprising:

at at least one of the authorized devices, using the group key of the set of keys corresponding to the group of which the authorized device is a member.

Claim 59 (new): The method according to claim 52 and wherein each group key of the set of keys is assigned an initial value, and said initial value can not be changed.

Claim 60 (new): The method according to claim 51 and wherein the authorized set comprises a plurality of maximal groups from the set of remaining groups, such that each maximal group is not a subset of any one of the set of remaining groups.

Claim 61 (new): The method according to claim 51 wherein the determining whether comprises receiving an identification of the at least one device.

Claim 62 (new): The method according to claim 51 and wherein each two devices of the plurality of authorized devices have at least one group key in common.

Claim 63 (new): The method according to claim 51 and wherein at least some of the authorized devices are not in communication with a central authorization facility after an initial manufacturing period.

Claim 64 (new): The method according to claim 52 and also comprising:

generating each of said group keys as a plurality of independently generated sets of group keys, wherein no group key of any one independently generated set is based, even in part, on any key of any other independently generated set.

Claim 65 (new): The method according to claim 52 and also comprising:

generating each of said group keys as a plurality of independently generated sets of group keys, wherein each group key is based, at least in part, pseudo-randomly on a source key.

Claim 66 (new): The method according to claim 52 and also comprising:

dividing the plurality of groups into a hierarchical set of groups, said hierarchical set of groups comprising a plurality of groups comprising at least a first group and a second group, each of said first group and said second group being associated with first and second group key generation information respectively; and

generating a least one group key in each of said first group and said second group using said associated group key generation information, wherein

said second group key generation information can be derived from said first group key generation information.